Introduction to SIEM

Cybersecurity

SIEM Day 1

Class Objectives

By the end of today’s class, you will be able to:

- Analyze logs and determine the types of data they contain, as well as the types of security events they can help identify.
- Isolate, identify, and correlate fields across raw log files.
- Design a correlation rule to notify when an event occurs.
- Make informed decisions about which SIEM vendor is best for an organization.

This week, we will move from offensive security to defensive security.

This Week...

Organizations must constantly determine whether the confidentiality, integrity, and availability of their data are being compromised.

For example

If an attacker were attempting to brute force their way into an an online auction company's admin website to steal information, the company would need to identify the activity before sensitive data and confidentiality were breached.

Over the next two weeks we will learn about SIEM (pronounced “sim”) technology, which organizations use to monitor and identify security incidents.

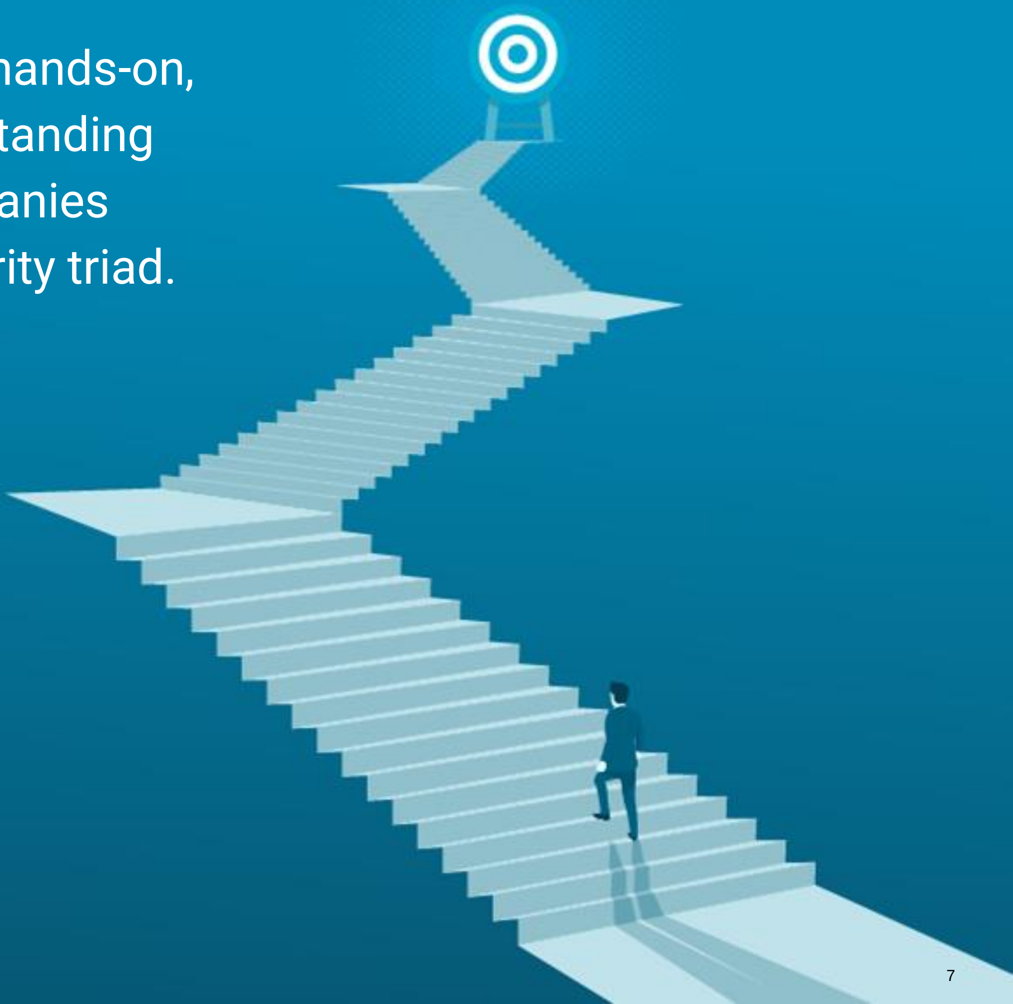
This Week...

You will play the role of a security operations center (SOC) manager at an online military products organization called Omni Military Products (OMP).

OMP recently experienced several security-related events that put their organization at risk.

As the new SOC manager, you will use SIEM tools and technologies to protect OMP from a variety of security events.

While the next two weeks will be very hands-on, today will focus on conceptual understanding and the business decisions that companies must make to maintain the cybersecurity triad.



Introduction to Continuous Monitoring

As the new SOC manager, you will be tasked with using SIEM tools and technologies to protect OMP from a variety of security events.

(Source)

Continuous monitoring, also known as information security continuous monitoring (**ISCM**), is the processes and technologies used to detect information security risks associated with an organization's operational environment in real time.

ISCM

ISCM provides real-time insight into the following:

The current state

of an organization’s networked assets.

Vulnerabilities

and threats that attack an organization’s networked assets.

Effectiveness

of security controls protecting an organization’s networked assets.

ISCM

As we know, organizations face many different threats.

For example:

- An employee can accidentally download malware onto their laptop, which can spread to an organization's network.
- A script kiddie can launch a denial of service attack against a web server.
- A nation state can attempt a code injection attack against an application.

Limiting ISCM

Organizations cannot protect against every single potential attack, as they may have:

Financial Limitations

Most modern monitoring tools and technologies are very expensive to install, deploy, and run. Organizations often have strict budgets that they have to maintain.

Staffing Limitations

While many monitoring tools have automated features, they often require humans to monitor and respond to detected issues.

Due to these limitations, organizations need to make business decisions to prioritize the types of security risks they will monitor against.

Prioritizing Risks to Monitor

Prioritizing Risks

Organizations consider the following factors when determining how to prioritize security risks:

- Compliance
- Financial Impact
- Reputational Impact
- Likelihood of Attack

Prioritizing Risk

Compliance: Depending on the industry a business is in, it may be required to monitor and analyze certain application and system activity.

For example

For example, to remain PCI-compliant, financial businesses that work with credit cards may be required to monitor their applications that manage financial data.

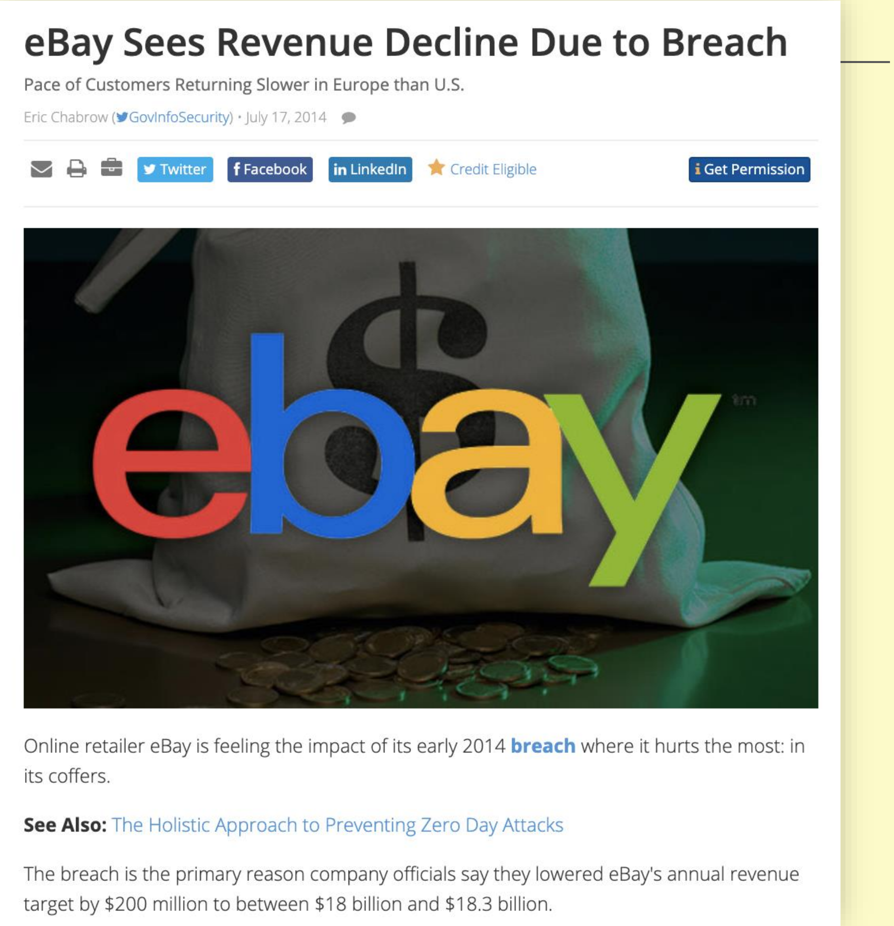
pci DSS COMPLIANT

Prioritizing Risk

Financial impact: How a system breach or shutdown can impact the financial performance of an organization.

For example

A business like eBay would likely prioritize monitoring their customer-facing application. The cost of this being compromised and taken offline would significantly affect their revenue.



eBay Sees Revenue Decline Due to Breach

Pace of Customers Returning Slower in Europe than U.S.

Eric Chabrow (GovInfoSecurity) • July 17, 2014

Online retailer eBay is feeling the impact of its early 2014 **breach** where it hurts the most: in its coffers.

See Also: The Holistic Approach to Preventing Zero Day Attacks

The breach is the primary reason company officials say they lowered eBay's annual revenue target by $200 million to between $18 billion and $18.3 billion.

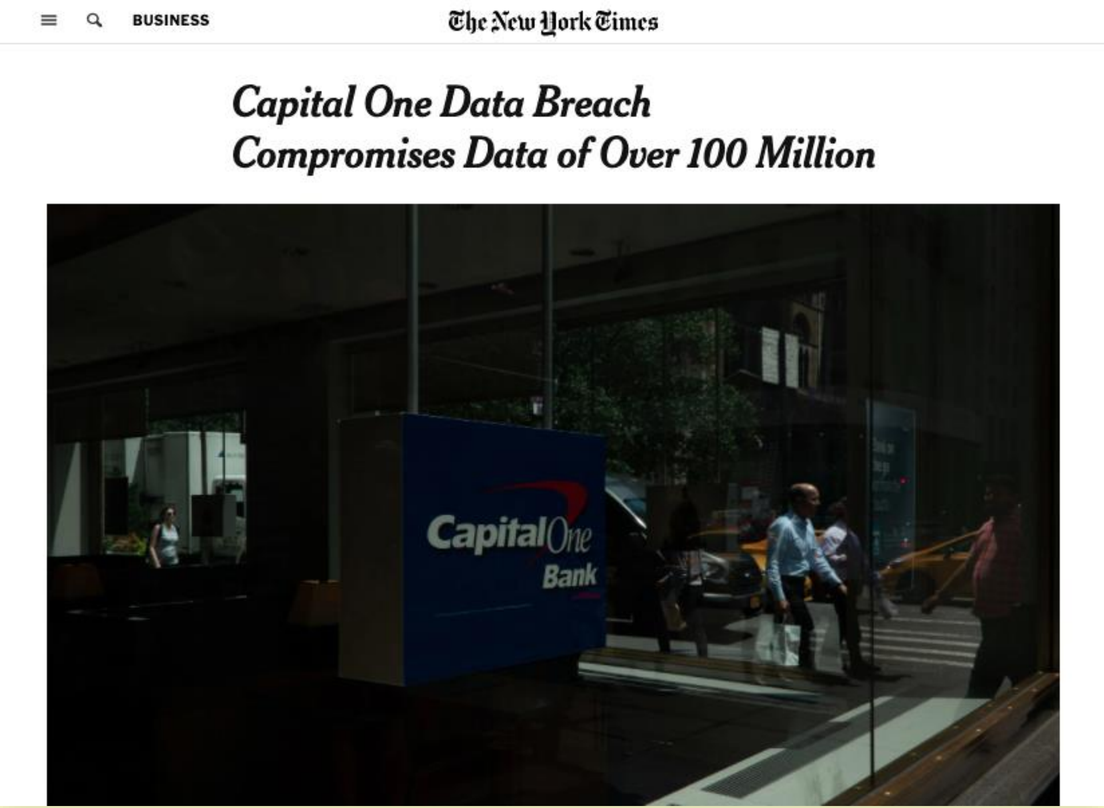
(Source)

Prioritizing Risk

Reputational impact:
How an incident would affect their reputation to customers.

For example

For example, an online banking provider would monitor their security controls of their customer financial data. If their customer data were breached, their reputation could be significantly affected.



Capital One Data Breach Compromises Data of Over 100 Million

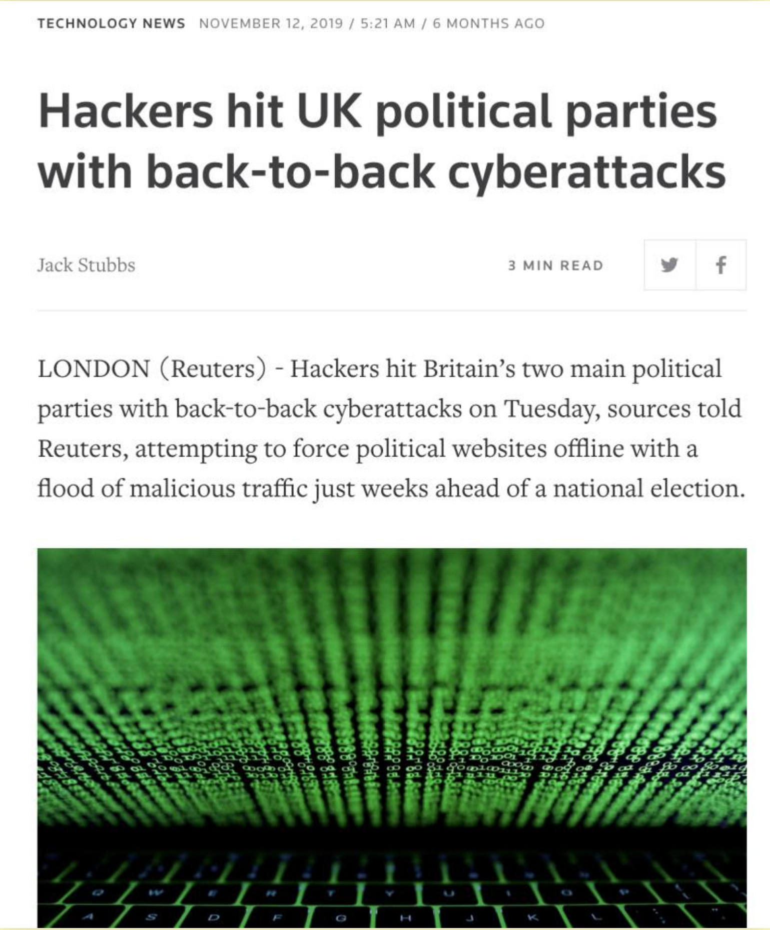
(Source)

Prioritizing Risk

Likelihood of attack: While there are many types of security risks that can occur, some are more likely than others.

For example

For example, politically-associated businesses that have public-facing websites are particularly at risk of denial of service attacks. Given this higher likelihood, these organizations should prioritize monitoring for DOS attacks.



TECHNOLOGY NEWS NOVEMBER 12, 2019 / 5:21 AM / 6 MONTHS AGO

Hackers hit UK political parties with back-to-back cyberattacks

Jack Stubbs

3 MIN READ

LONDON (Reuters) - Hackers hit Britain's two main political parties with back-to-back cyberattacks on Tuesday, sources told Reuters, attempting to force political websites offline with a flood of malicious traffic just weeks ahead of a national election.

(Source)

Organizations must decide for themselves which factors to consider when prioritizing risks.

Activity: Monitoring Your Assets

In this activity, you will analyze the types of security events and rank them based on risk to the organization.

Suggested Time:
7 Minutes

Time’s Up! Let’s Review.

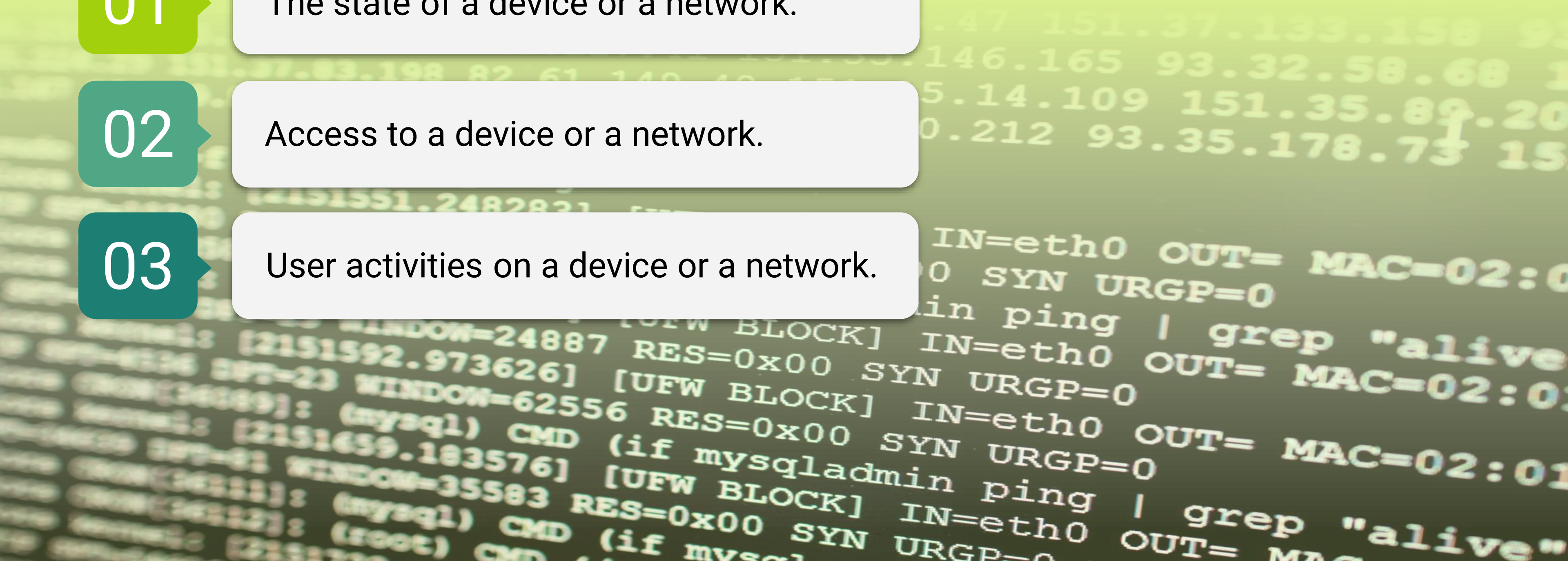
Logs, Logs, and more Logs

After organizations decide what kind of events they want to monitor, they need to decide *how* to monitor them.

Logs are the most common organizational method for monitoring. These are collections of entries that record individuals events occurring on a device or network.

Logs

While log entries were originally designed to assist with troubleshooting system issues, they later proved useful to security professionals as a source of insight into:



01 The state of a device or a network.

02 Access to a device or a network.

03 User activities on a device or a network.

Types of Logs

Due to the quantity of networking and security assets and devices, logs come from a variety of sources:

- Operating system logs
- Application logs
- Networking device logs
- Security device logs

Types of Logs

Operating system logs are created on devices such as Linux and Windows systems.

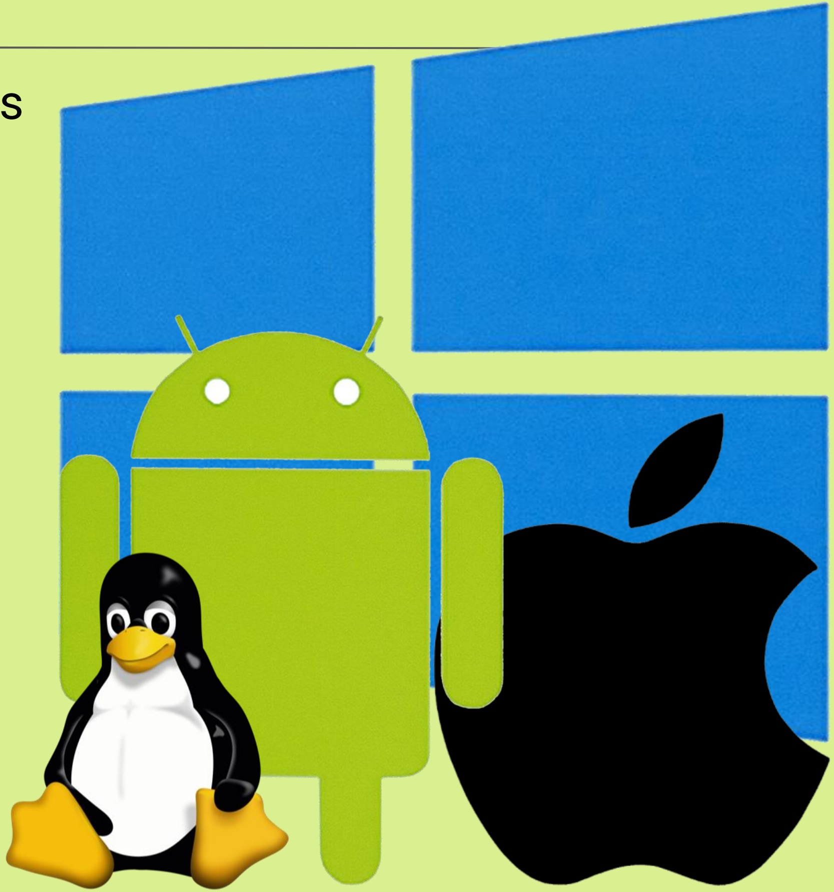
Security events that can be identified by these logs include:

Security access events

Such as an unauthorized user attempts to view privileged data, such as a company payroll file.

Security permissions events

Such as a user attempts to give themselves permissions to view and edit a privileged file.



Types of Logs

Application logs are created by devices such as Apache and IIS (Internet Information Services) servers.

Security events that can be identified by these logs include:

Application access events

Such as a brute force attempt to log into an administrative account on a web application.

Fraud events

Such as a user on a financial application attempting to transfer a large sum of funds to a suspicious external account.

Microsoft IIS

APACHE
HTTP SERVER PROJECT

Types of Logs

Networking device logs are created on devices such as routers, switches, and DHCP/DNS servers.

Security events that can be identified by these logs include:

Administrative events

Such as a network administrator accidentally opening a port allowing unauthorized traffic into a network.

Network security events

Such as a DHCP starvation attack in which the DHCP server receives thousands of requests in a short period of time, consuming all available IP addresses.

Types of Logs

Security device logs are created on devices such as IDS/IPS, firewalls, endpoint devices, and honeypots.

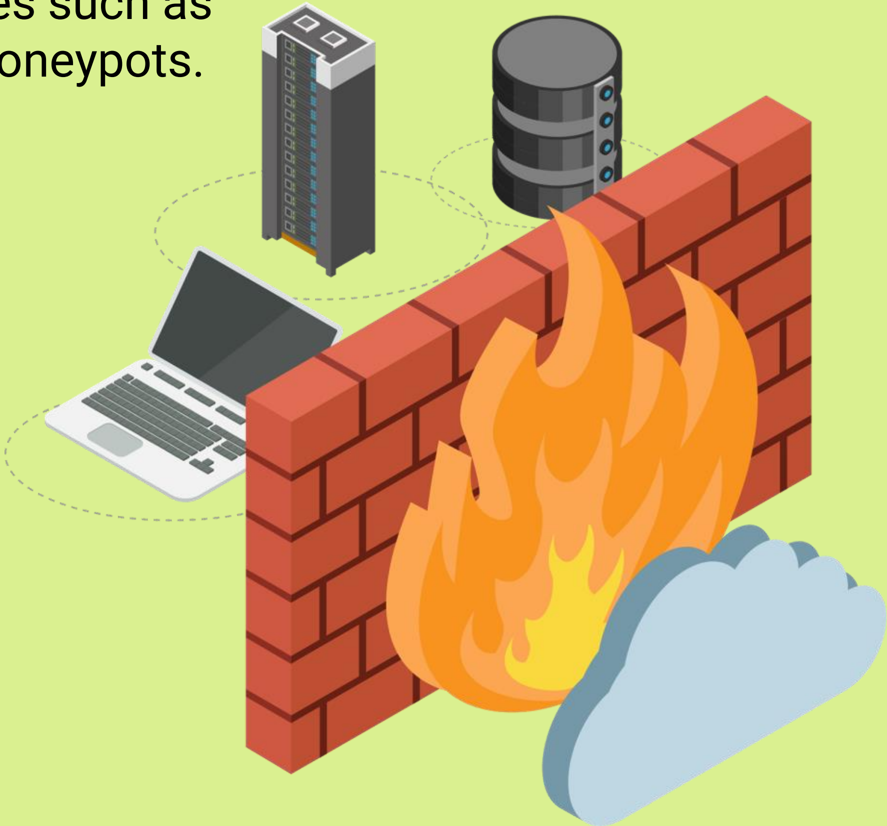
Security events that can be identified by these logs include:

Endpoint events

Such as a user accidentally downloading malware onto their laptop from a phishing email.

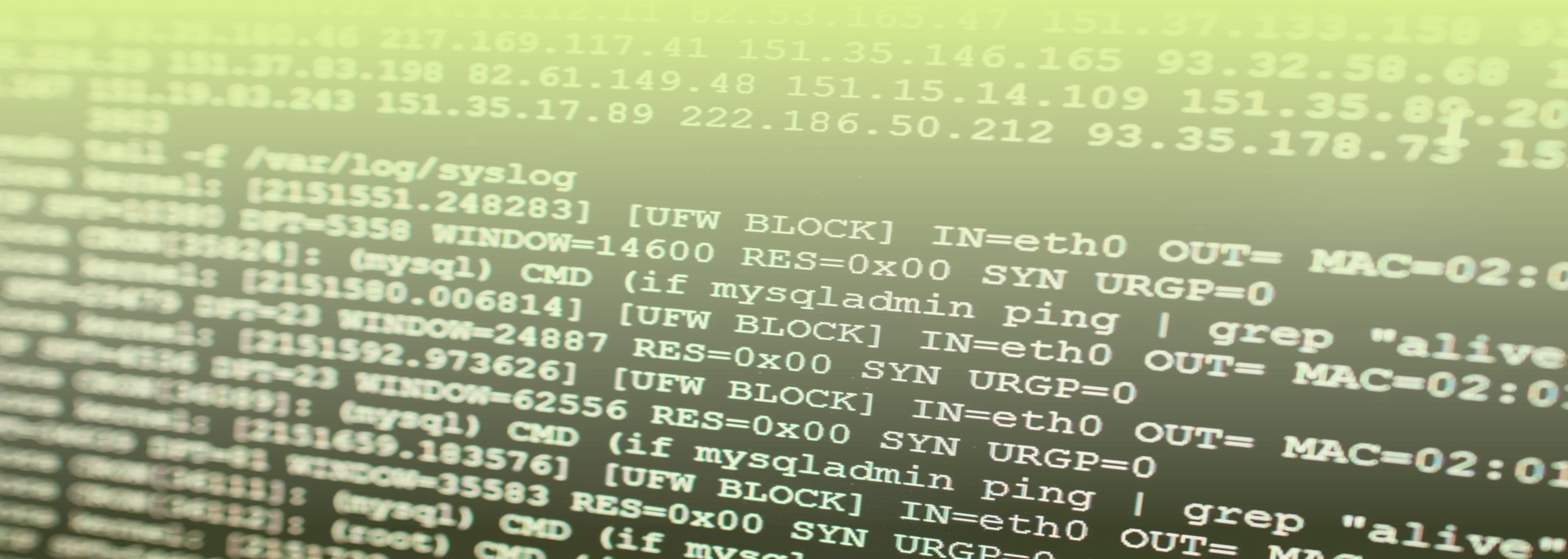
IDS signature events

Such as a packet with an illegal TCP flag combination being identified by an IDS.



Logs

While this is not a complete list of all the possible logs that security professionals use, students should be familiar with these types of logs and the types of security events they can help identify.



```
14.1.112.11 82.53.165.47 151.37.133.158
93.33.180.46 217.169.117.41 151.35.146.165 93.32.58.68
151.37.83.198 82.61.149.48 151.15.14.109 151.35.89.20
151.19.83.243 151.35.17.89 222.186.50.212 93.35.178.73 15
tail -f /var/log/syslog
kernel: [2151551.248283] [UFW BLOCK] IN=eth0 OUT= MAC=02:0
DPT=5358 WINDOW=14600 RES=0x00 SYN URGP=0
CRON[35824]: (mysql) CMD (if mysqladmin ping | grep "alive
kernel: [2151580.006814] [UFW BLOCK] IN=eth0 OUT= MAC=02:0
DPT=23 WINDOW=24887 RES=0x00 SYN URGP=0
kernel: [2151592.973626] [UFW BLOCK] IN=eth0 OUT= MAC=02:0
DPT=23 WINDOW=62556 RES=0x00 SYN URGP=0
CRON[36089]: (mysql) CMD (if mysqladmin ping | grep "alive
kernel: [2151659.183576] [UFW BLOCK] IN=eth0 OUT= MA
DPT=81 WINDOW=35583 RES=0x00 SYN URGP=0
(mysql) CMD (if mysql
(root) CMD
```

Activity: What is this Log?

In this activity, you will analyze and categorize various log types.

Suggested Time:
7 Minutes

Time’s Up! Let’s Review.

Countdown timer

15:00

(with alarm)

Log Aggregation and Normalization

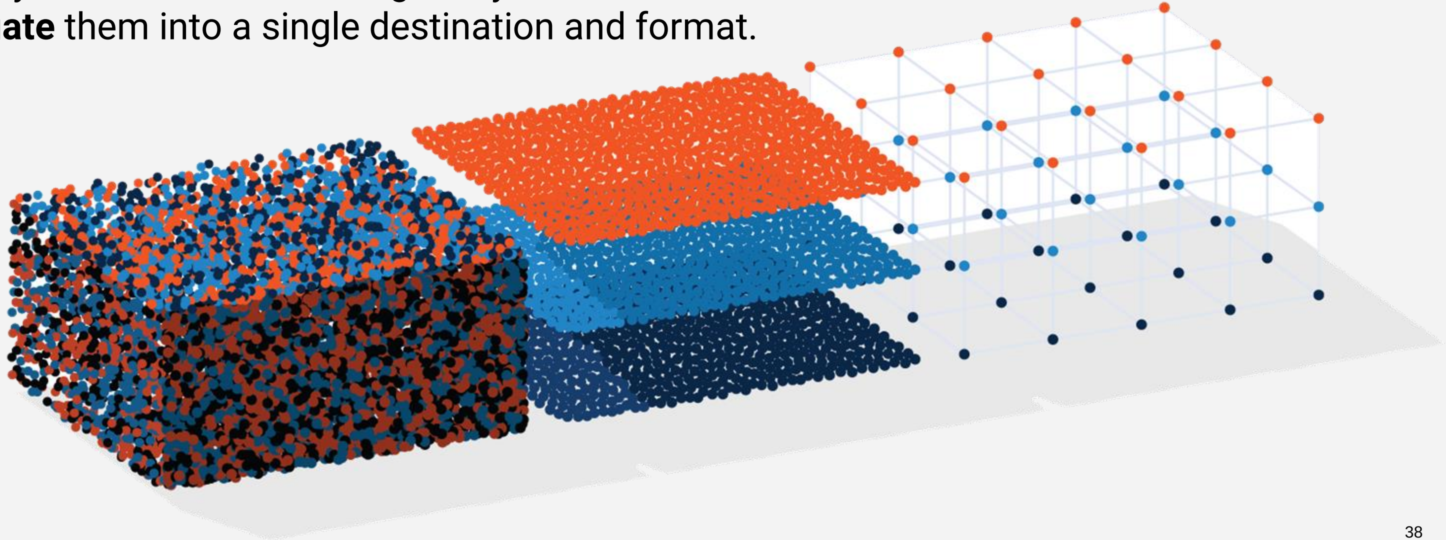
Whole Lotta Logs

The amount of incoming logs from various sources can be overwhelming.

For example

if a business wants to monitor suspicious logins on their Linux servers, they may have to monitor a variety of Linux servers and distributions.

They'd want to identify all the Linux server logs they have available and **aggregate** them into a single destination and format.



Log aggregation is the identification and collection of logs from multiple computing sources.

Log Aggregation

Logs from different sources, even if they are logging similar data, are often created in different formats.

Log 1:

```
User TJones Successfully Authenticated to 10.182.12.35 from client 43.10.8.22
```

Log 2:

```
43.182.12.35 New Client Connection 84.10.8.22 on account: PSmith: Success
```

Log Parsing

Log parsing is the process of converting the single string of data and into structured data.

Log 1:

```
User | TJones | Successfully Authenticated | to | 10.182.12.35 | from client | 43.10.8.22
```

Log 2:

```
43.182.12.35 | New Client Connection | 84.10.8.22 | on account: | PSmith | : Success
```

By separating the values, each field can be categorized and rearranged to match a uniform structure.

Log Normalization

Log normalization is the process of standardizing fields in data from different sources and formats so it can be analyzed together.

Key: User | Destination IP | Source IP

Log 1:

```
User TJones Successfully Authenticated to 10.182.12.35 from client 43.10.8.22
```

Log 2:

```
43.182.12.35 New Client Connection 84.10.8.22 on account: PSmith: Success
```

Activity:
Log Aggregation and Normalization

In this activity, you will aggregate and normalize various logs by identifying the fields contained within the log files.

Suggested Time:
7 Minutes

Time’s Up! Let’s Review.

Log Correlation

Log Correlation

We can use log correlation to detect security events.

- Individual log entries often do not indicate security events alone.
- Analyzing multiple log entries together can help us detect security events and patterns of suspicious behavior.
- Log correlation connects multiple log entries to make raw data into useful information.
- Different log entries can come from the same source or different sources.

Log Correlation

While this single entry may not seem suspicious...

```
[10/12/2019 04:32:03 PM]   41.34.54.233  user=testerA "Login Failed"
```

Log Correlation

The following log entries correlated together indicate a potentially suspicious security event, such as a brute force attack.

```
[10/12/2019 04:32:03 PM]   41.34.54.233  user=testerA "Login Failed"
[10/12/2019 04:32:04 PM]   41.34.54.233  user=testerA "Login Failed"
[10/12/2019 04:32:05 PM]   41.34.54.233  user=testerA "Login Failed"
[10/12/2019 04:32:07 PM]   41.34.54.233  user=testerA "Login Failed"
[10/12/2019 04:32:08 PM]   41.34.54.233  user=testerA "Login Failed"
[10/12/2019 04:32:09 PM]   41.34.54.233  user=testerA "Login Failed"
[10/12/2019 04:32:10 PM]   41.34.54.233  user=testerA "Login Failed"
[10/12/2019 04:32:11 PM]   41.34.54.233  user=testerA "Login Failed"
[10/12/2019 04:32:12 PM]   41.34.54.233  user=testerA "Login Failed"
[10/12/2019 04:32:13 PM]   41.34.54.233  user=testerA "Login Failed"`
```

Correlation Rules

Log correlation identifies security events by using correlation rules.

01

Correlation rules are the logic used to identify security events.

02

Correlation rules look at a sequence of events that can identify a potential security issue.

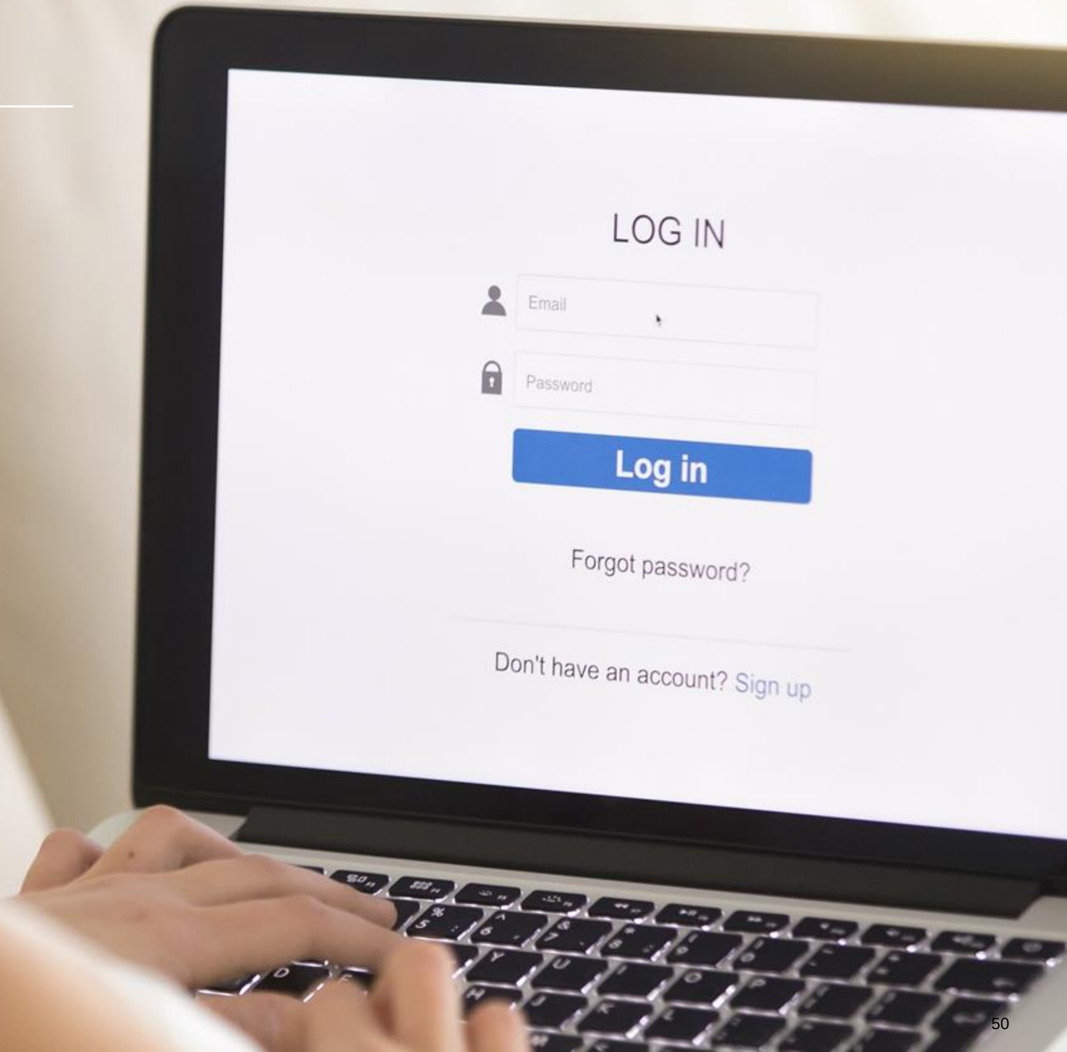
03

Correlation rules are often dynamic, which means they can change depending on how effective they are.

Correlation Rule

For the list of logs we just looked at, we can create a correlation rule that detects an attempted brute force attack if all the following are true:

- More than three failed logins
- From the same user
- From the same IP address
- Within a five-minute period



Once a rule is triggered, we need to decide what action to take.

The most common response is an **alert**.

A **correlation alert** is a notification that correlation rules have been met and an event was detected.

Correlation Alerts

Correlation alerts can have multiple delivery methods.

- Displays on the screen at a SOC.
- Notifications sent with phone calls, text messages, or emails.
- Alerts are often designed to notify multiple individuals for faster response.
- Alerts typically provide high-level details of the reason for the alert.

Correlation Rule and Alert

If the following is detected:

- ⚠ More than three failed logins
- ⚠ From the same user
- ⚠ From the same IP address
- ⚠ Within a five-minute period

Send the following alerts:

- **Phone call to SOC manager**
- **Email to SOC distro list**

Activity: Correlation Rules

In this activity, you will create correlation rules that will be used to identify if an attack is happening.

Suggested Time:
10 Minutes

Time’s Up! Let’s Review.

SEM + SIM = SIEM

Security Monitoring

Organizations take the following steps to monitor against security events:

01 Organizations decide **what to monitor** by prioritizing the risks to their business.

02 Organizations decide **how to monitor**, which is typically accomplished by logs.

03 Organizations **aggregate**, **parse**, and **normalize** logs so they can be analyzed together.

04 Organizations **correlate** logs with rules to alert when a security event is detected.

Security professionals use security information and event management (SIEM) to simplify and manage monitoring security events.

SIEM

SIEM is made up of two types of software:

Security information management (SIM)

Primarily focused on log management and involves collecting logs in a central location for later analysis.

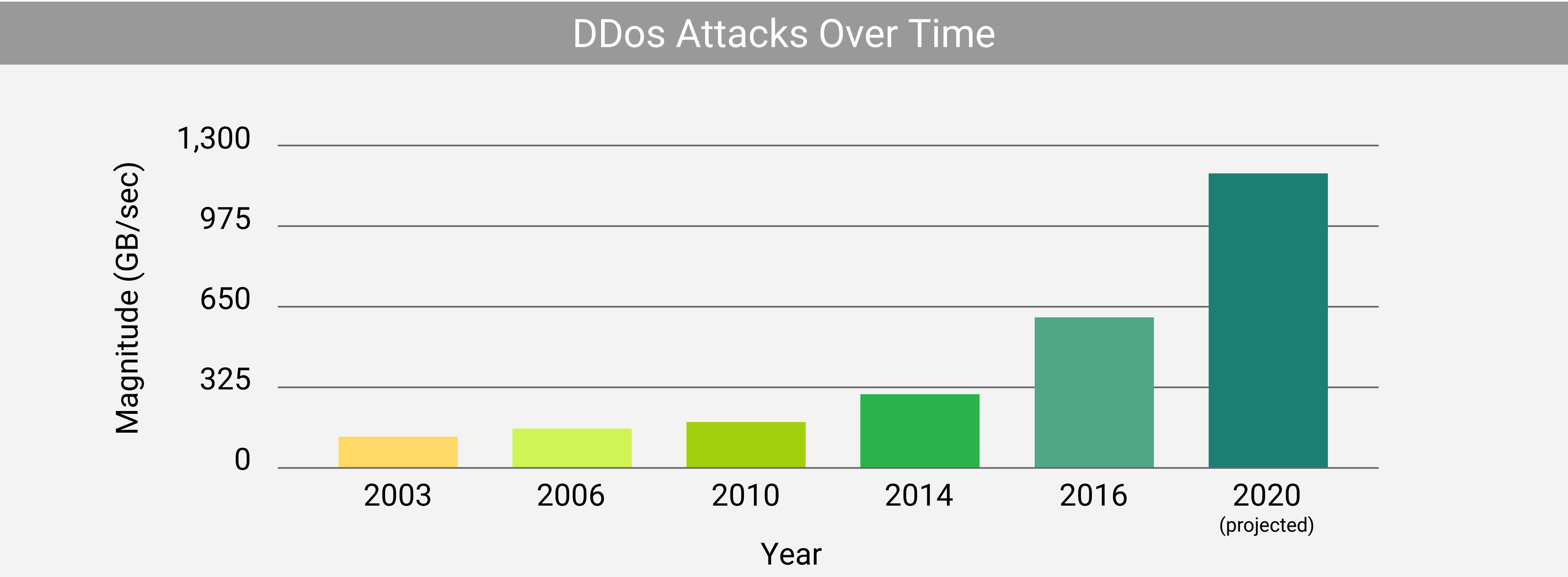
Security event management (SEM)

Primarily focused on event monitoring and involves identifying, evaluating, and correlating logs to determine security events and create alerts.

SIEM combines the technologies of SIM and SEM to collect, organize, and analyze logs to detect security-related events across an organization's technology infrastructure.

SIEM

SIEM can also be used to visualize data related to security events in order to simplify data interpretation.



SIEM can assist organizations with the steps covered in today’s lesson to implement an effective monitoring solution.

Organizations need to decide what to monitor by prioritizing the risks to their business.

How can SIEM help?

A SIEM can...

....look at historical data to determine how often a security has has occurred. This data can help an organization prioritize monitoring decisions.

Organizations decide how to monitor, which is typically accomplished by logs.

How can SIEM help?

SIEM are...

...made of smart devices that assist security departments with forwarding and collecting logs from various sources.

Organizations aggregate, parse, and normalize multiple logs so they can be analyzed together.

How can SIEM help?

One of SIEM’s greatest strengths...

...is their automation of aggregation, parsing, and normalization. When logs are loaded into SIEM, they are automatically parsed and normalized, with all the field headers identified. This reduces the manual work of parsing and identifying all fields.

Organizations correlate these logs with correlation rules to alert when a security event or suspicious activity is detected.

How can SIEM help?

Most SIEM have an...

...easy-to-use rule correlation designer, which makes it simple for SOC employees to manage the creation, editing, and viewing of correlation rules.

There are many SIEM vendors and products available, each offering different solutions.

Considering a Vendor

Organizations should consider the following when selecting a vendor:

Consideration	Reason
Cost	While cost is always a consideration when selecting a SIEM vendor, how an organization is billed can also be a consideration.
Ease of implementation and use	Organizations should research how challenging a SIEM vendor's solutions will be to set up and manage.
Log compatibility	Organizations should confirm that the SIEM vendor is able to accommodate every type of log the business is required to monitor.
SIEM features	While every SIEM vendor claims to have the most advanced and user-friendly features, organizations should review each vendor's features and assess which will best serve their business goals.

Activity: Choosing a SIEM Vendor

In this activity, you will choose the SIEM vendor that is the best fit for your organization.

Suggested Time:
7 Minutes

Time’s Up! Let’s Review.

The End